Please amend Claims 1 to 6, 8 and 10 to 15, and add new Claims 16 to 29 as shown below. The claims, as pending in the subject application, now read as follows:

1. (Currently amended) A method for the secure printing of print data from a client application residing on a data network to an interface device ~~a set top box~~ which has a printer, said interface device ~~set top box~~ residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

determining whether a secure communication path exists between said client application and said interface device ~~set top box~~;

transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said interface device ~~set top box~~; and

sending said print data from said interface device ~~set top box~~ to said printer for printing.

2. (Currently amended) A method according to Claim 1, wherein the step for determining whether said [[a]] secure communication path exists between said client application and said interface device ~~set top box~~ includes the use of a secure protocol between said client application and said cable head end, and between said cable head end and said interface device ~~set top box~~.

3. (Currently amended) A method according to Claim 2, wherein the step for determining whether said [[a]] secure communication path exists between said client application and said interface device ~~set top box~~ further includes a confirmation through said secure protocol, that said cable head end is a secure location, and a confirmation, through said secure protocol, that said interface device ~~set top box~~ is a secure location.

4. (Currently amended) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said interface device ~~set top box~~ includes sending said print data from said client application to said cable head end in a device-independent format, transforming said print data from said device-independent format to a rasterized format which corresponds to said printer, and then sending said print data in said rasterized format from said cable head end to said interface device ~~set top box~~ for printing on said printer.

5. (Currently amended) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said interface device ~~set top box~~ includes encrypting said print data, sending said encrypted print data from said client application to said cable head end, sending said encrypted print data from said cable head end to said interface device ~~set top box~~, decrypting said print data, and sending the decrypted print data to said printer for printing.

6. (Currently amended) A method according to Claim 3, wherein said confirmation that said interface device ~~set top box~~ is a secure location is sent from said interface device ~~set top box~~ to said cable head end.

7. (Original) A method according to Claim 3, wherein said confirmation that said cable head end is a secure location is sent from said cable head end to said client application.

8. (Currently amended) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said interface device ~~set top box~~ includes transforming, by said client application, said print data from said device-independent format to a rasterized format which corresponds to said printer, sending said print data in said rasterized format from said client application to said cable head end, and then sending said print data in said rasterized format from said cable head end to said interface device ~~set top box~~ for printing on said printer.

9. (Original) A method according to Claim 2, wherein said secure protocol is a secure sockets layer protocol.

10. (Currently amended) A method according to Claim 2, wherein the step for determining whether said [[a]] secure communication path exists between said client application and said interface device ~~set top box~~ includes the transmission of at least one certificate from said interface device ~~set top box~~ to said cable head end and the transmission of at least one certificate from said cable head end to said client application.

11. (Currently amended) A method for the secure printing of print data from a client application residing on a data network to an interface device ~~a set top box~~ which has a printer, said interface device ~~set top box~~ residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of;

generating print data in said client application;

determining that a secure communication path exists between said client application and said cable head end upon receipt through a secure protocol of a confirmation from said cable head end that said cable head end is a secure location;

sending, in response to a determination that said secure communication path exists, said print data from said client application to said cable head end in a device-independent format;

transforming in said cable head end, said print data from said device-independent format to a rasterized format which corresponds to said printer;

determining that a secure communication path exists between said cable head and said interface device ~~set top box~~ upon receipt, through a secure protocol, of a confirmation from said interface device ~~set top box~~ that said interface device ~~set top box~~ is a secure location; and

sending, in response to a determination that said secure communication path exists, said print data in said rasterized format from said cable head end to said interface device ~~set top box~~ for printing on said printer.

12. (Currently amended) A method for the secure printing of print data from a client application residing on a data network to an interface device ~~a set top box~~ which has a

printer, said interface device ~~set top box~~ residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

transforming, in said client application, said print data from said device-independent format to a rasterized format which corresponds to said printer;

encrypting, in said client application, said print data in said rasterized format;

sending said encrypted print data in said rasterized format from said client application to said cable head end;

sending said encrypted print data in said rasterized format from said cable head end to said interface device ~~set top box~~; and

decrypting, in said interface device ~~set top box~~, said print data in said rasterized format for printing on said printer.

13. (Currently amended) An apparatus for the secure printing of print data from a client application residing on a data network to an interface device ~~a set top box~~ which has a printer, said interface device ~~set top box~~ residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, comprising:

a program memory for storing process steps executable to perform a method according to any of Claims 1 to 12; and

a processor for executing the process steps stored in said program memory.

14. (Currently amended) Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for the secure printing of print data from a client application residing on a data network to an interface device ~~a set top box~~ which has a printer, said interface device ~~set top box~~ residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 12.

15. (Currently amended) A computer-readable medium which stores computer-executable process steps, the computer-executable process steps to achieve the secure printing of print data from a client application residing on a data network to an interface device ~~a set top box~~ which has a printer, said interface device ~~set top box~~ residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 12.

16. (New) A method according to Claim 1, wherein said interface device is a set top box.

17. (New) A method according to Claim 11, wherein said interface device is a set top box.

18. (New) A method according to Claim 12, wherein said interface device is a set top box.

19. (New) An apparatus according to Claim 13, wherein said interface device is a set top box.

20. (New) Computer-executable process steps according to Claim 14, wherein said interface device is a set top box.

21. (New) A computer-readable medium according to Claim 15, wherein said interface device is a set top box.

Same as 1

22. (New) A method for the secure printing of print data on a network, said method comprising the steps of:

rendering print data;

determining whether a secure communication path to an interface device which has a printer exists;

transmitting, in response to a determination that said secure communication path exists, said rendered print data to said interface device via a network; and

sending said rendered print data from said interface device to said printer for printing.

23. (New) A method according to Claim 22, wherein the step for determining whether said secure communication path to said interface device exists, includes the use of a secure protocol between a client application and a cable head end, and between said cable head end and said interface device.

24. (New) A method according to Claim 23, wherein the step for determining whether said secure communication path to said interface device exists, further includes a confirmation through said secure protocol, that said cable head end is a secure location, and a confirmation, through said secure protocol, that said interface device is a secure location.

25. (New) A method according to Claim 23, wherein the step for determining whether a secure communication path to said interface device exists, includes the transmission of at least one certificate from said interface device to said cable head end and the transmission of at least one certificate from said cable head end to said client application.

26. (New) An apparatus for the secure printing of print data on a network, comprising:

a program memory for storing process steps executable to perform a method according to Claim 22; and

a processor for executing the process steps stored in said program memory.

27. (New) Computer-executable process steps stored on a computer-readable medium, said computer-executable process steps for the secure printing of print data on a network, said computer-executable process steps comprising process steps executable to perform a method according to Claim 22.

28. (New) A computer-readable medium which stores computer-executable process steps, the computer-executable process steps to achieve the secure printing of print data on a network, said computer-executable process steps comprising process steps executable to perform a method according to Claim 22.

29. (New) A method according to Claim 22, wherein the step for rendering print data includes rasterizing the print data by using a printer driver corresponding to said printer.